UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,884	05/17/2006	Osamu Aoki	P06,0069	5969

26574 7590 06/29/2009

SCHIFF HARDIN, LLP
PATENT DEPARTMENT
6600 SEARS TOWER
CHICAGO, IL 60606-6473

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
06/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/579,884	AOKI ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-29, 33-35, and 39-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-29,33-35 and 39-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/579884 is presented for examination by the examiner. Claims 31 and 36-38 have been canceled. Claims 39-42 have been added. Claims 17-29, 33-35, and 30-42 remain pending.

Response to Amendment

Claim Objections

The previous claim objections have been overcome by amendment.

Claim Rejections - 35 USC § 101

The previous 101 rejection has been rendered moot by cancellation of claims.

Claim Rejections - 35 USC § 112

The previous 112 rejection has been rendered moot by cancellation of claims.

Response to Arguments

Applicant's arguments filed 5/26/09 have been fully considered but they are not persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., local events contributing to the creation of both the first and second profile) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The independent claims do not require the first and second profile to be created from a single local event. Moreover, there is nothing in the claim that requires both profiles to even be created for a single event. All that is required is that the system can differentiate between whether a user is or is not logged into the computer and make a decision as to the authorization of an instruction by comparing it to one of two profiles based on a user's presence. The combination of McCallam and Sekiguchi provide this teaching. Per McCallam, if a user is logged into the computer the system collects parameters about that login (profile) and compares it to an established user profile (0069). It does this when a user is logged in. However, McCallam suggests that attacks can be detected anywhere on the LAN (0066). Sekiguchi teaches that a system can protect itself against attacks not only from users but other computers (col. 9, lines 56-65). Sekiguchi creates a log file of instructions which originate from another computer. The system converts the log data into security management information. This is synonymous to a profile and the collected parameters of McCallam. These parameters which are indicative of the operation requested are compared to an acceptable policy in order to judge the operation's authorization. If Applicant desires the claim to be narrowly interpreted as meaning the system creates both profiles on a single operation by a single local user,

then those limitations should be brought into the claims. The teachings of the specification will not be read into the claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 17-29, 33-35, and 39-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCallam et al. (US 2004/0230832 A1) hereinafter McCallam, in view of Sekiguchi (USP 6,711,687).

As per claims 17, 29, and 39, McCallam teaches the limitation of "an operation-receiver for receiving instruction data for executing said operation" (page 4, paragraph 0047) as the user input manager receives user inputs and directs those inputs to the data analyzer for execution.

In addition, McCallam teaches the limitations of "a first profile-creator for creating a first profile from said instruction data related to the operation for which instruction data was received by said computer", "a first profile-storer for storing said first profile that was created by said first profile-creator", "a second profile-creator for identifying a user

that executed said operation by said instruction data, and creating a second profile related to the operation executed by said user", and "a second profile-storer for storing, according to user, said second profiles created by said second profile-creator" (page 6, paragraph 0066) as the detection manager contains software routines, data storage, and processing means to detect an IW attack anywhere on the LAN. Detection may be based on a number of potential activities that are monitored by the detection manager. For example, insider misuse can be detected when an authorized user performs an unauthorized, or perhaps, infrequent operation that may raise the suspicion that the authorized user's computer is being misused. In another example, user profile data may be stored in a database and may be used to detect an intrusion. The user may have access to a particular database but has not accessed the database for over a year. A sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

Finally, McCallam teaches the limitation of "a score-calculator for comparing said instruction data with at least one profile that is stored in said first profile-storer or in said second profile-storer, and calculating a score for determining whether said operation is an unauthorized operation" (page 6, paragraph 0068) as the comparator may examine data at network devices and compare the data to a predefined condition and (page 6, paragraph 0069) the comparator compares the collected parameters to an established user profile that reflects normal operation of the network device.

McCallum is silent in disclosing that the first profile is compared to when said computer is not logged into a user account. Examiner interprets this limitation to be a

remote access to said computer by something other than a normal user logged into the computer. This is in contrast to the second profile condition which states comparison to the instruction with that of a locally logged in user account. Therefore, Examiner makes the distinction between the first and second profile as the former being created when an outside entity attempts to initiate a process on a computer remotely, and the latter being created when a local user attempts to initiate a process on the computer locally. McCallum teaches the second profile and comparison as indicated above. McCallum is silent in explicitly teaching the condition to which the first profile is created and compared. Sekiguchi teaches this limitation in his system when it is able to detect threats posed by outside (remote) computing devices which has no user account associated with them (col. 9, lines 54-65 and col. 10, lines 1-10). Sekiguchi system creates a profile and stores security management information for comparing access between computers without user intervention. Specifically this is to protect computers which do not have to have a user logged in. This reads on the newly amended limitation of comparing instruction data with first profile when there is not user account logged in. It would have been obvious to use this type of profiling and comparing with McCallum because new types of threats could be detected and blocked. Being able to stop threats at a computer without a user logged in greatly improves the response of the system. It is obvious to combined known methods which yield predictable results. Combining McCallum and the teaching of Sekiguchi as the first type of profile would allow the system to stop illegal user attempts and remote computer attempts of access on the system.

With respect to claim 18, McCallam teaches the limitations of "a first log-data-storer for storing log data of said computer", "a second log-data-storer for storing log data according to a user of said computer", "wherein said first profile-creator references said first log-data-storer when creating said first profile", and "wherein said second profile-creator references said second log-data-storer when creating said second profile" (Fig. 5E; page 6, paragraphs 0067 and 0069) as a data storage device 379 containing the user profiles 400 and trend of the performance parameters 410.

With respect to claims 19, 33, and 40, McCallum teaches the limitation of "a login-detector for executing a process for detecting whether a certain user is logged into said computer; wherein when said login-detector detects that a certain user is logged in, said second profile-creator creates a second profile related to said user" (0070) as the database may store the local version of the user profile. The database may also store historical values of the computer performance parameters and the user profile.

With respect to claim 20, McCallum teaches the limitation of "said login-detector executes detection processing at specified intervals while said computer is in operation" (0079).

As per claims 21, 34, and 41, Examiner supplies the same rationale as recited in the rejection of claim 17, to incorporate as the first profile the teaching of Sekiguchi.

With respect to claim 22, McCallum teaches the limitation of "said login-detector executes detection processing at specified intervals while said computer is in operation" (0079) as the service manager that determines a periodicity of monitoring computers and other network devices for indication of intrusion and misuse.

As per claims 23, McCallum is silent in teaching a third profile-creator for creating a third profile related to an operation executed by a user that is identified as a first-time user, when the user executing said operation by said instruction data is identified as a first-time user operating said computer for the first time; and

a third profile-storer for storing third profiles that are created by said third profile-creator; wherein said *score-calculator* uses at least one profile that is stored in said third profile-storer instead of said second profile-storer to determine whether said operation is an unauthorized operation. Sekiguchi teaches these limitations as storing security information for new users to verify their access attempts on the network (col. 9, lines 36-55). It would have been obvious to profile new users because the system has yet to analyze their behavioral patterns. This would greatly increase the systems ability to correctly deal with new users while patterns are detected. It is obvious to combine known method which produced predictable results. One of ordinary skill in the art would have been motivated to create a separate profile for new users in order to deal with them efficiently until a pattern of behavior could be established.

With respect to claim 24, McCallum is silent in explicitly teaching an operation-record-storer for storing, according to user, totals related to at least one of the following: number of logins to said computer, operation time that said computer has been operated, or number of days said computer has been operated; and

a first-time-user-judgment mechanism for referencing said operation-record-storer, and determining that a user executing said operation is a first-time user using said computer for the first time when said totals do not satisfy preset reference values;

and wherein said third profile-creator creates a third profile for an operation executed by a user that is determined to be a first-time user by said first-time-user- judgment mechanism; and

said score-calculator uses at least one profile stored in said third profile-storer when said first-time- user-judgment mechanism determines that a user is a first- time user to determine whether said operation is an unauthorized operation.

Sekiguchi teaches an operation-record-storer for storing, according to user, totals related to at least one of the following: number of logins to said computer, operation time that said computer has been operated, or number of days said computer has been operated [col. 9, lines 40-42; access restriction information is kept for new users for a predetermined amount of time]; and

a first-time-user-judgment mechanism for referencing said operation-record-storer, and determining that a user executing said operation is a first-time user using said computer for the first time when said totals do not satisfy preset reference values (col. 9, lines 40-41);

and wherein said third profile-creator creates a third profile for an operation executed by a user that is determined to be a first-time user by said first-time-user-judgment mechanism [col. 9, lines 36-38; access restriction applied to new users]; and

said score-calculator uses at least one profile stored in said third profile-storer when said first-time- user-judgment mechanism determines that a user is a first- time user to determine whether said operation is an unauthorized operation (col. 9, line 37; specific security level is used). Sekiguchi teaches these limitations as storing security

information for new users to verify their access attempts on the network (col. 9, lines 36-55). It would have been obvious to profile new users because the system has yet to analyze their behavioral patterns. This would greatly increase the systems ability to correctly deal with new users while patterns are detected. It is obvious to combine known method which produced predictable results. One of ordinary skill in the art would have been motivated to create a separate profile for new users in order to deal with them efficiently until a pattern of behavior could be established.

As per claim 25, McCallum teaches said score-calculator calculates a score by calculating a deviation between said instruction data and data that is stored in said profiles (0070).

As per claim 26, McCallum teaches an operation-stopper for executing a process for stopping said operation when said score value exceeds a reference value (0069).

With respect to claim 27, McCallum teaches the limitation of "a warning-process for executing a process for displaying a warning on an operation screen of said computer, or generating a warning alarm on said computer, when said score exceeds a reference value" (page 6, paragraph 0066) as a sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

With respect to claim 28, McCallam teaches the limitation of "a warning-notification-transmitter for sending a notification warning to an administration server operated by an administrator of said computer that there is a possibility of an unauthorized operation, when said score exceeds a reference value" (page 6,

paragraph 0068) as the comparator may examine data at network devices and compare the data to predefined condition. The detection manager may provide an alert or other means of notifying the security server.

With respect to claims 35 and 42, McCallum teaches the limitation of "said login-detector executes detection processing at specified intervals while said computer is in operation" (0079).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431